Preprint
UCRL-CONF-204799

Systems Analysis of Safeguards Effectiveness in a Uranium Conversion Facility

H. A. Elayat, H. E. Lambert, and W. J. O'Connell

This article was submitted to the 45th Annual Meeting of the Institute of Nuclear Materials Management, Orlando, FL, July 18-22, 2004

June 17, 2004

U.S. Department of Energy

Lawrence
Livermore
National
Laboratory

SYSTEMS ANALYSIS OF SAFEGUARDS EFFECTIVENESS IN A URANIUM CONVERSION FACILITY

Hatem A. Elayat, Howard Lambert, and William J. O'Connell
Lawrence Livermore National Laboratory
7000 East Ave., Livermore, CA 94550-9234, USA (925) 422-8983

ABSTRACT:
The U.S. Department of Energy (DOE) is interested in developing tools and methods for potential U.S. use in designing and evaluating safeguards systems. For this goal several DOE National Laboratories are defining the characteristics of typical facilities of several size scales, and the safeguards measures and instrumentation that could be applied. Lawrence Livermore National Laboratory is providing systems modeling and analysis of facility and safeguards operations, diversion path generation, and safeguards system effectiveness. The constituent elements of diversion scenarios are structured using directed graphs (digraphs) and fault trees. Safeguards indicator probabilities are based on sampling statistics and/or measurement accuracies. Scenarios are ranked based on value and quantity of material removed and the estimated probability of non-detection. Significant scenarios, especially those involving timeliness or randomly varying order of events, are transferred to simulation analysis. Simulations show the range of conditions encountered by the safeguards measurements and inspections, e.g., the quantities of intermediate materials in temporary storage and the time sequencing of material flow. Given a diversion campaign, simulations show how much the range of the same parameters observed by the safeguards system can differ from the base-case range. The combination of digraphs, fault trees, statistics and simulation constitute a method for evaluation of the estimated benefit of alternate or additional safeguards equipment or features. A generic example illustrates the method.

INTRODUCTION

The function of a safeguards system on a chemical conversion plant is in general terms to verify that no useful nuclear material is being diverted to use in a nuclear weapons program. The IAEA now considers all highly purified uranium compounds as useful [1].

The U.S. Department of Energy (DOE) is interested in developing instruments, tools, strategies, and methods that could be of use in the application of safeguards to the front end of the fuel cycle. A current DOE project [2] is examining safeguards approaches for generic conversion facilities with a range of scales of throughput. Lawrence Livermore National Laboratory (LLNL) is providing systems modeling and analysis of plant operations, diversion paths, safeguards verifications, and safeguards system effectiveness.

Figure 1 shows the framework for performing systems analysis for evaluating the effectiveness of a safeguard system for a uranium conversion facility. Inputs from other laboratories include the facility and safeguards system characterization. The digraph-fault tree analysis is at the heart of the process. It structures possible diversion activities in a diversion scenario together with the safeguards measures and activities relevant to the diversion scenario. Then it incorporates possible failure modes of the safeguards measures and develops a fault tree for the safeguard system in this situation. Among the inputs to the fault tree are the analysis of the inspector's verification of the facility material declarations. Specifically these inputs are the probabilities of detection of various diversion activities meant to influence the facility's declared nuclear material balance. Outputs of the digraph-fault tree analysis are the probability of success, quantity, and value

This work was performed under the auspices of the U.S. Department of Energy by the University of California, Lawrence Livermore National Laboratory under Contract No. W-7405-Eng-48.

of the material removed in the diversion scenarios. The most attractive diversion scenarios are selected for time-domain simulation. The simulations track the uranium flow through the facility. The simulations include normal operation, intermediate storage, normal variations of input flow, and diversion scenarios.

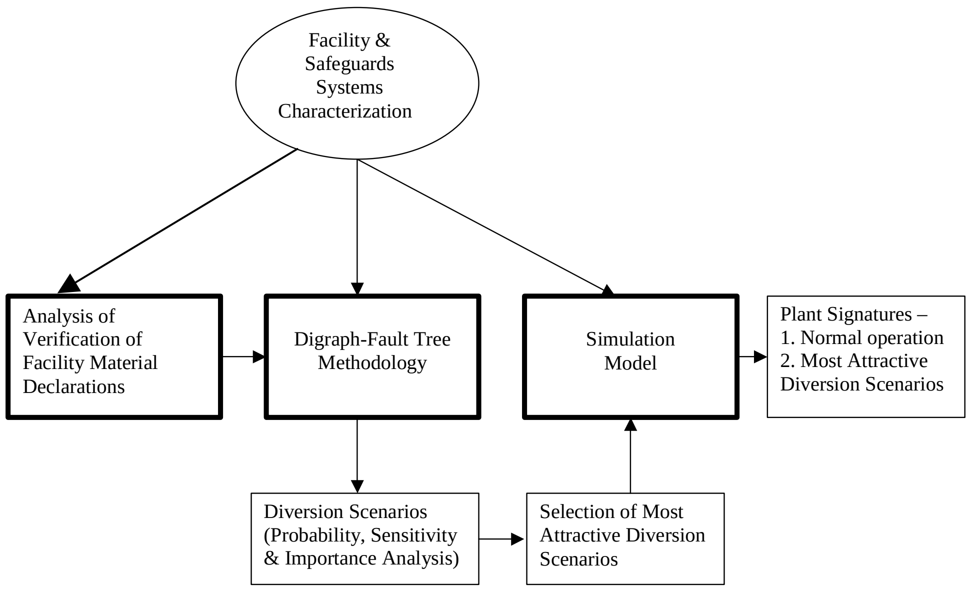

Figure 1. Framework for performing systems analysis for evaluating the effectiveness of a safeguard system for a uranium conversion facility

Simulation outputs are the time series of material outputs, which illustrate the data signatures of normal operation and diversion schemes. The simulation model can be used as an inspection tool. The model can be stored on the laptops of inspectors while inspection of the plant is occurring. The simulation model can be run to conduct "what if" scenarios and can be helpful in identifying data signatures that are indicative of diversion.

DIGRAPH-FAULT TREE METHODOLOGY

The purpose of the digraph-fault tree methodology is to systematically generate and analyze diversion scenarios. Diversion scenarios for this study describe how a facility could divert a significant amount of purified uranium without detection. The basic steps to the methodology are:

- Describe system to be analyzed – flows, amounts, unit processes etc
- Describe safeguards measures to be implemented by the Facility Operator and by Inspectors
- List removal nodes (Points of Diversion)
- Define diversion scenarios for each removal node
- Construct a directed graph for each diversion scenario
- From the directed graph, construct a fault tree that describes how the diversion scenario can occur (top event is failure of the safeguards system to detect the diversion)
- Fault tree evaluation
    1. Find the modes of failure for each diversion scenario called min cut sets
    2. Compute the probability of safeguards system failure for each diversion scenario
    3. Conduct Sensitivity and Importance Analysis
- Determine the most attractive diversion scenarios for simulation.

Previous use of the digraph fault tree methodology for safeguards effectiveness assessment
Lawrence Livermore National Laboratory, in the late 70's, developed a procedure for the U.S. Nuclear Regulatory Commission to assess the effectiveness of a material control and accounting systems at nuclear fuel cycle facilities. [3,4]. The digraph fault tree methodology was used in this study. A test bed design that was a modification of a section of the Barnwell plant in South Carolina was used to illustrate the methodology.

Many elements of the 70's study described above apply to analysis of fuel cycle facilities for international safeguards and hence for this study. However, the 70's study did not consider diversion strategies by facilities, which is important for the current study. For example, uranium could be diverted in one part of the process and the facility could make misdeclarations to conceal the fact that material is missing. Modeling diversion strategies makes the fault tree process much more complicated and is considered in this study and illustrated by an example.

Overview of the digraph fault tree methodology
A digraph (directed graph) is an influence diagram that depicts the interrelationship of process variables and events within a system, represented by nodes in the digraph. The digraph depicts the information flow associated with generation of anomalies as the facility attempts to divert material and/or conduct concealment activities so that the diversion is not detected. Anomalies are potential indicators of diversion. **Detection paths** in the digraph represent the generation of anomalies. The information to generate a detection path in the digraph is based on the physical or stimulus variables in figure 2. The basic starting point is diversion of material from the facility. The immediate impact is that the inventory of material in the facility decreases. Depending upon the strata and material form diverted, physical variables such as flow, concentration, mass, radioactive emissions may change. As the material is removed, the facility may conduct concealment activities (re-entry from the bottom right in figure 2). These may generate other anomalies that the agency may detect such as discrepancies and inconsistencies in material accounting.

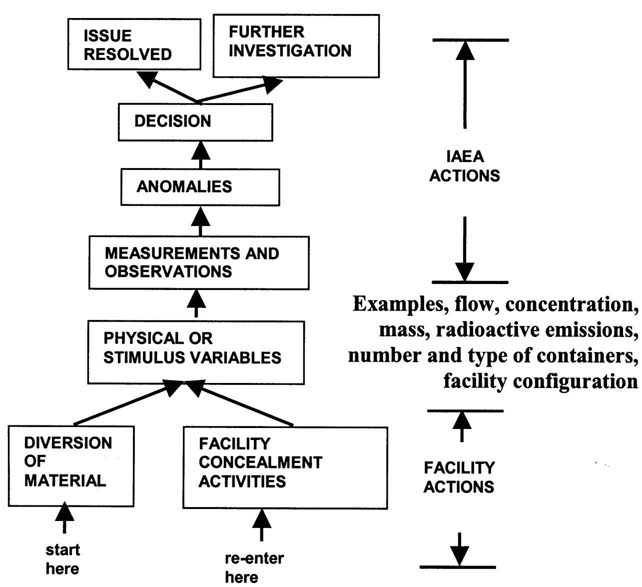

Figure 2 – Information flow for generation of detection paths in the digraph

The fault tree is derived from the digraph as follows. As material removal and/or concealment activities occur, anomalies activate detection paths in the digraph. Each detection path in the digraph must fail in order for the facility to successfully divert material without detection. Material removal from the facility is the first basic event generated in the fault tree. Then all other basic events (also known as bottom events, root causes or primary failures) in the fault tree describe all the ways detection paths can fail to detect diversion and subsequent concealment activities that disguise the diversion. Basic events include for example, records falsification, misdeclarations, material substitution, measurement uncertainties, random component failures, use of unapproved containers or equipment, component tampering, broken seals and inspector error. As the facility conducts additional concealment activities, other detection paths in the digraph must fail that result in the generation of additional AND gates in the fault tree.

The unique combinations of basic events that cause the fault tree top event to occur are the diversion paths (called min cut sets in reliability). The min cut sets are obtained by Boolean algebra manipulation of the fault tree. Once the min cut sets are found and the probability of the basic events determined, the probability of successful diversion could be computed by the use of standard fault tree analysis evaluation techniques, as illustrated in [3,4]. Sensitivity and importance analysis of the fault tree can be conducted. As an example of a sensitivity analysis, one could evaluate the fault tree assuming that material accounting measures are in place only and that containment and surveillance measures have failed. An importance analysis could depict the most likely min cut sets and basic events that contribute to successful diversion. The most attractive diversion scenarios are identified as candidates for simulation.

Simplified Example

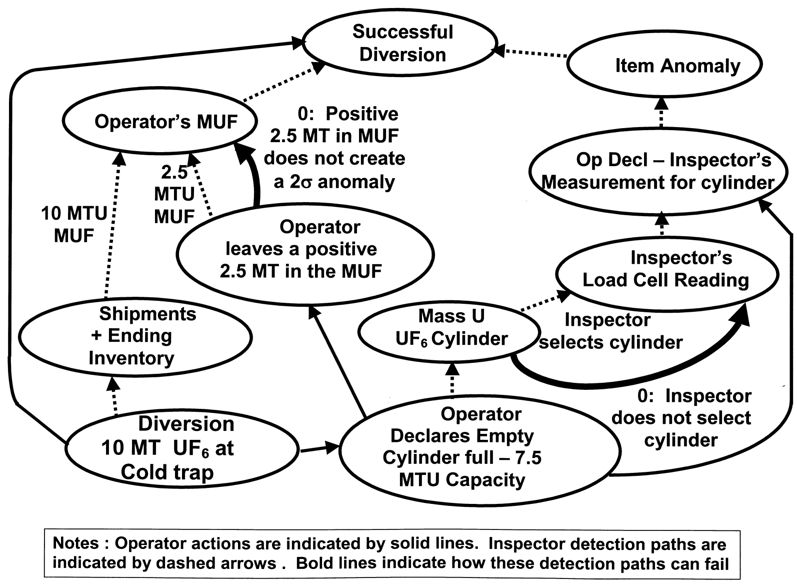

Figure 3 – Digraph for Diversion of 10 MT of UF_6 at a cold trap

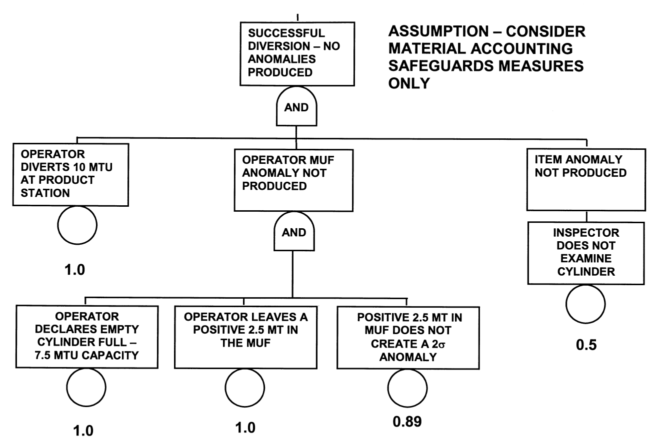

Figure 4 – Fault Tree for Successful Diversion of 10 MT of Uranium

We consider diversion of 10 MTU (as UF_6) from a cold trap at a uranium conversion facility. We give credit to material accounting measures only and consider only the annual physical inventory verification in which the inspector examines the operator declared mterial unaccounted for (MUF). In addition, we assume that 50% of the UF_6 cylinders are inspected, weighed and surveyed. We assume that the facility declares the non-existence of a gross defect by declaring an empty UF_6 cylinder full. A cylinder contains 7.5 MT of U (MTU) as UF_6. In addition, we assume that the operator leaves 2.5 MTU in the MUF. The actual MUF reported is then a statistical variable distributed about 2.5 MTU. The simplified digraph for this diversion scenario is shown in figure 3. The top node is successful diversion. Two nodes in the digraph – an operator's declared MUF and an item anomaly – represent two indicators of diversion. There are three detection paths indicated by dashed lines. The first detection path is represented on the left side (operator's declared MUF of 10 MTU) and is the first path to be considered since the node represents material removal. The 10 MTU anomaly fails by the operator making a misdeclaration. The remaining 2.5 MTU MUF anomaly is represented by the second detection path in digraph. The probability that the MUF measurements will not produce a warning indicator at the 2 σ level, is 0.82 (see statistical analysis below). This is the probability that this detection path will fail. If the inspector examines the misdeclared cylinder, then he would detect an empty cylinder – represented by the third detection path in the digraph. However, if the inspector does not examine the cylinder, then the third detection path would also fail. Bold lines indicate the events that fail all three paths. The fault tree is shown in figure 4. The fault tree shows for successful diversion to occur is that all three detection paths in the digraph must fail. There is one min cut set of order 5 to this fault tree as indicated by the five basic events indicated by circles. The probability of this min cut set is (1 x 1 x 1 x 0.82 x 0.5) = 0.41 – it is assumed that intentional facility actions occur with probability 1.

STATISTICAL EVALUATION OF VERIFICATION MEASUREMENT PLANS

Several possible operator measures to conceal a missing amount of uranium from the MUF indicator involve making misdeclarations in the operator's material balance measurements. These include gross defects, partial defects, and bias defects. Of course, the smaller the individual defects, the greater is the number of containers needed to cover a significant quantity of uranium. Further measures include leaving some positive balance in the MUF and asserting it is just a statistical fluctuation. Verification measurement plans for inspections will select a random sample of the containers for measurement by several methods. For example, one non-destructive analysis and one more accurate destructive analysis method may be in use. To detect a pattern of many very small bias defects, the inspector aggregates all the differences between the inspector's measurements and the operator's declared measurements into the difference statistic D [5]. The inspector also examines the facility's stated MUF and the MUF – D statistic.

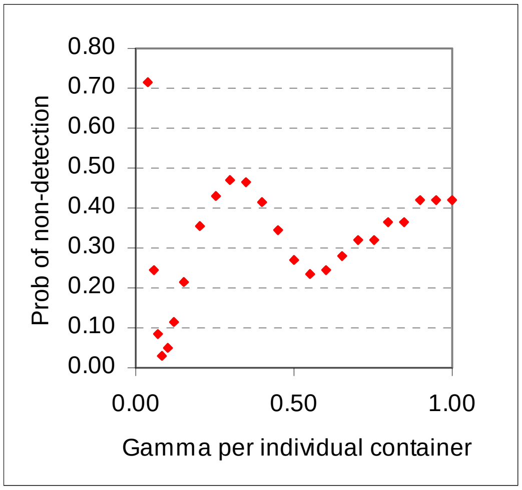

Fig. 5. Probability of nondetection of a goal quantity in one year, using two measurement methods, and based on a desired probability of 0.5 or less.

An IAEA algorithm selects a sampling plan for each stratum of throughput or inventory based on the amount of material in throughput or inventory, the desired probability of detection of diversion of a significant quantity, and the measurement accuracies of the operator's and inspector's instruments. The next step is to determine the probability of detection for the given sampling plan. To do this we extend Lu et al [6]. An example with a desired non-detection probability of 0.5 or less is shown in Fig. 5. This hypothetical example involves an assumed goal quantity of 7.5 MTU, a normal outgoing quantity of 97.5 MTU in 80 containers, thus a minimum of 7 defect containers at 100% defect to achieve the goal quantity.

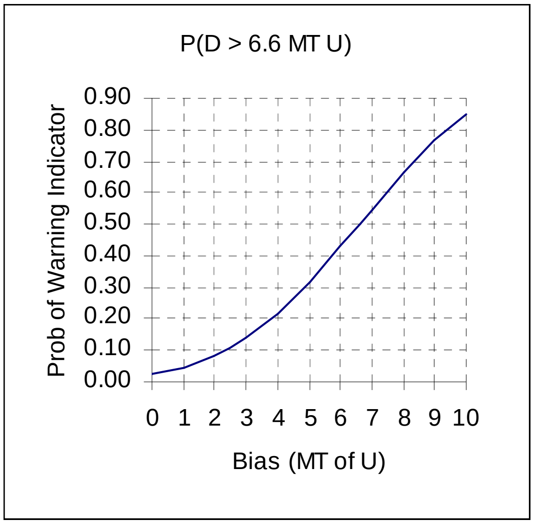

Figure 6. Probability of a warning indicator of 2σ, for a given total σ = 3.3 MT for the difference statistic.

If a diverter decides to cover only half of a significant quantity from one stratum and half from a second stratum, the probability of non-detection in a single stratum is higher, but the overall probability of non-detection remains approximately the same.

To examine for a pattern of bias defects, the inspector combines the differences in measurements in a stratum, and then combines strata differences weighted by the stratum size. The quantities of uranium in the annual material balance for MUF for the generic small facility are typically 100 MT input, 100 MT output of product and waste, and 30 MT each in the beginning and ending inventories. To detect a bias of 10 MT with 3σ accuracy requires a $\sigma = 3.3$ MT or 1.27%. This is feasible, based on ITV values [7] if we assume that values for clean uranium scrap may be applied to uranium ore concentrates. Reducing the random uncertainty may require more sampled measurements than for the partial defects sampling plan.

A threshold level of 3σ and a probability of 50% of getting an alarm signal for a bias of 10 MT leaves smaller probabilities of getting an alarm signal for smaller biases. Boyer [8] proposes an alarm level of 2σ. This causes a few percent of false alarms from honest biases and measurement statistics, so it is a signal for further investigation rather than a definite alarm. But it does raise the warning signal with reasonable probability for deliberate biases of only fractions of a significant quantity. See Fig. 6.

If the difference statistic has $\sigma = 3.3$ MT, then the facility's and the inspector's σ for the same subset of measured items are expected to be about 2.3 MT each, and likely dominated by the systematic rather than the random errors. For the digraph example above, the probability of a warning indicator for a deliberate MUF excess of 2.5 MT is 0.18. This 2.5 MT is 25% of a significant quantity, and its probability of detection is 36% of the overall goal of 50% probability of detection of a significant quantity.

As an alternate diversion strategy, the 2.5 MT could be concealed by a deliberate bias of 2.5 MT. Then the probability of a warning indicator from the D statistic is 0.11, or 22% of the overall goal of 50% probability of detection of a significant quantity.

SIMULATION MODEL

An Extend® simulation model was developed for the generic conversion facility shown in "Uranium conversion process for a small size plant" Figure 3 of reference [9]. Extend is a graphical, interactive, general-purpose simulation program for both discrete event and continuous modeling [10]. The simulation model consists of eleven modules, each representing part of the conversion process, from receipt of material

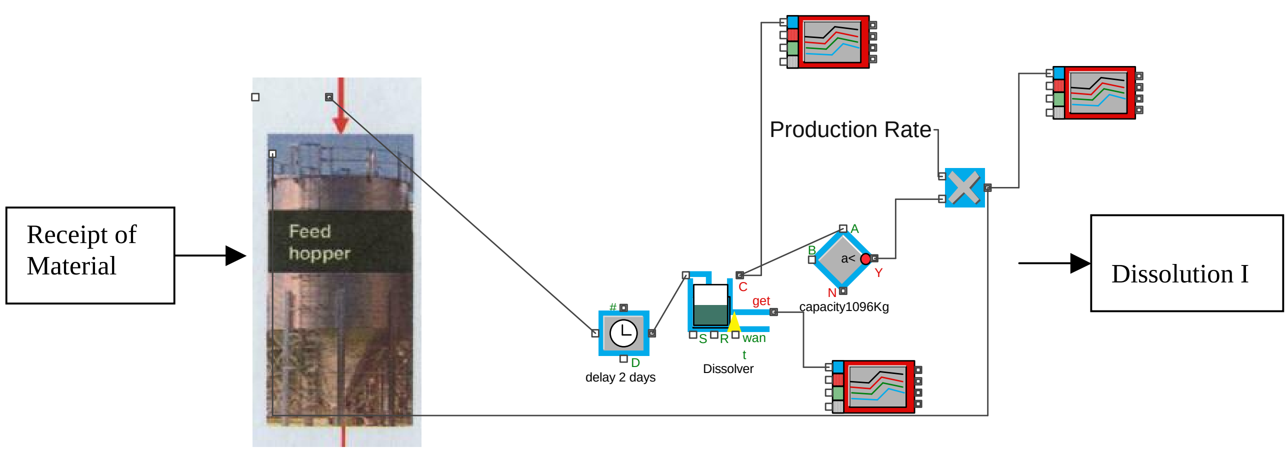

Figure 7. Feed Hopper Module in Extend Simulation Model

to UF_6. The Feed Hopper module is shown in Figure 7. It consists of iconic-blocks representing what is being modeled, the Feed Hopper, processing time, Dissolver, capacity constraint, and charts to monitor the flow of material at every stage.

Extend (v.6) was used to model the continuous process. Input parameters to the simulation model were sized to match plant throughput, and were allowed to vary by 5%. The simulation was run for one year with a time step of one day. Figure 8 shows the plant signature when 10 MTU of UF_6 was diverted at the cold trap during a one-year period, it also shows the total amount of yellow cake used during production throughout the year as well as the amount of UF_6 produced. Figure 9 shows the amount of liquid waste produced throughout the year, in Waste streams r, Raffinate, and Organics measured in Kg. Similar plots were

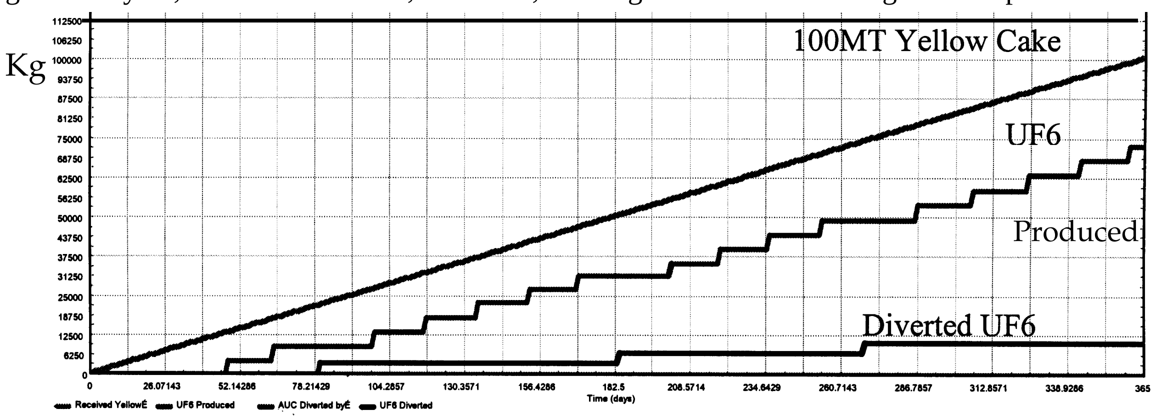

Figure 8. Diversion of 10MT of UF6 from Cold Trap Throughout the Year

generated for solid waste. The inspectors can use these simulation results, as a tool, to identify abnormal signatures, which might indicate the diversion of UF_6. As an example of an abnormal signature, consider the

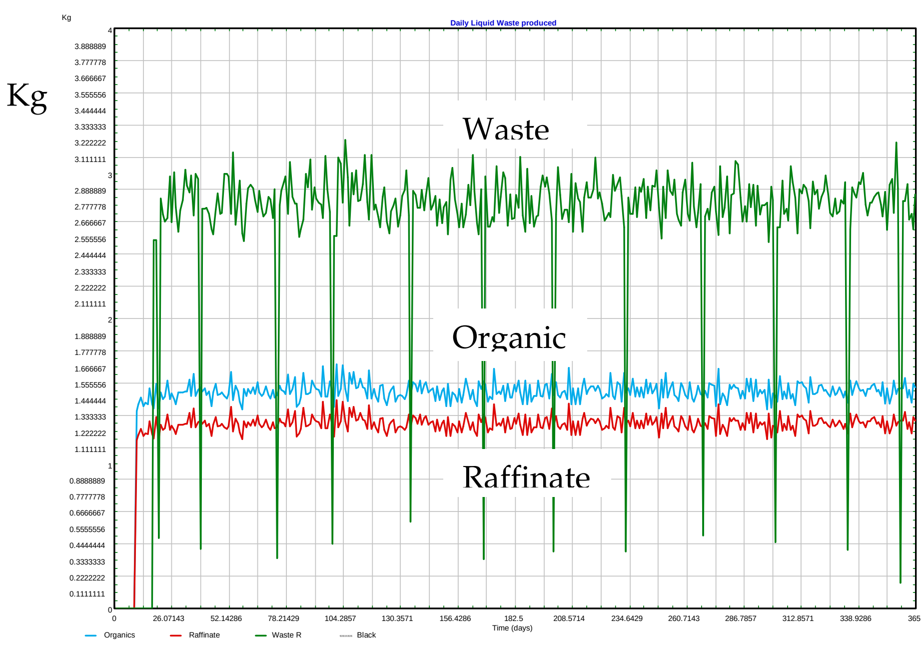

Figure 9. Daily Liquid Waste Products

diversion scenario shown in figure 8. UF_6 is produced in batches. During the year, 3 diversions of UF_6 occurred. When diversion occurs, it takes longer to produce a batch of UF_6 as indicated by the length of the time interval to produce the batch.

REFERENCES

[1] Jay Doo, Davis Hurt, Robert Fagerholm and Neil Tuley, *Safeguards Approach for Natural Uranium Conversion Plants*, paper No. 292 in Proceedings of the Institute of Nuclear Material Management, 44th Annual Meeting, Phoenix, AZ, July 13-17, 2003.

[2] B. Boyer, et al, *U.S. DOE Efforts to Enhance Conversion and Enrichment Plant Safeguards*, presented at the 7th International Conference on Facility Operations-Safeguards Interface, February 29-March 4, 2004, Charleston, SC.

[3] H. E. Lambert, J. J. Lim and F.M. Gilman, *A Digraph-Fault Tree Methodology for the Assessment of Material Control Programs*, NUREG/CR-0777, Lawrence Livermore National Laboratory, UCRL-52710. May 1979.

[4] H. Lambert and J. Lim, *The Modeling of Adversary Action for Safeguards Effectiveness Assessment*, UCRL-79217, Lawrence Livermore National Laboratory, June 1977, Presented at the INMM conference, June 29,1979, Arlington, VA.

[5] *IAEA Safeguards Technical Manual, Part F: Statistical Concepts and Techniques, Volume 3*, IAEA-TECDOC-261, Vol. 3, 1982, available on IAEA Publications web site.

[6] M.-S. Lu, T. Teichmann, and J. B. Sanborn, *An Integrated Approach for Multi-Level Sample Size Determination*, BNL-64739, Brookhaven National Laboratory, 1997.

[7] H. Aigner et al., *International Target Values 2000 for Measurement Uncertainties in Safeguarding Nuclear Materials*, IAEA Report STR-327, April 2001; also published in JNMM, V. 30 Nr. 2, 2002.

[8] B. Boyer, private communication, Brookhaven National Laboratory, May 12, 2004.

[9] R. L. Faulkner et al., *Oak Ridge efforts to enhance conversion plant safeguards*, presented at the 45th Annual Conference of the Institute of Nuclear Materials Management INMM, July 18-22, 2004, Orlando, Florida.

[10] Bob Diamond, *Extend: A Library-based, hierarchical, multi-domain modeling system*, Proceedings of the 1993 Winter Simulation Conference, December 12-15, 1993, Los Angeles, CA.